IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. PHILLIP R. DURACHINSKY, Defendant.	)	INDICTMENT CASE NO. 1:18 CR 00022 Title 18, United States Code, Sections 1028A(a)(1), 1030(a)(2)(C), (a)(3), (a)(5)(A), (c)(2)(A), (c)(4)(A)(i)(I) and (c)(4)(B), 1343, 2251(a) and 2511(1)(b) and (4)(a), and 2

JUDGE OLIVER

GENERAL ALLEGATIONS

At all times material herein:

1. From in or around 2003 through on or about January 20, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY engaged in a scheme to access protected computers without permission.

2. During his more than thirteen years of accessing protected computers without the appropriate authorizations, Defendant accessed protected computers owned by local, state and federal governments, a police department, schools, companies and individuals.

3. Defendant developed computer malware later named "Fruitfly" and wrote variants capable of infecting computers running macOS and Windows operating systems.

4. Defendant installed the Fruitfly malware on thousands of computers ("Fruitfly victims").

5. The Fruitfly malware gave Defendant the ability to control a Fruitfly victim's computer by, among other things, accessing stored data, uploading files to a Fruitfly victim's computer, taking and downloading screenshots, logging a user's keystrokes and turning on the camera and microphone to surreptitiously record images and audio recordings.

6. In certain cases, the Fruitfly malware alerted Defendant if a user of an infected computer typed certain words associated with pornography. Defendant used the Fruitfly malware to watch and listen to Fruitfly victims without their knowledge or permission. He saved millions of images and regularly kept detailed notes of what he observed.

7. Defendant developed a control panel for the Fruitfly malware that ran on a computer in a residence in the Northern District of Ohio, Eastern Division. The control panel allowed Defendant to manipulate computers infected with the Fruitfly malware and had a visual interface that allowed Defendant to view live images and data from several infected computers simultaneously.

8. Defendant used his access to Fruitfly victims' computers to collect and save personal data from Fruitfly victims including tax records, medical records, photographs, internet searches performed, banking records and potentially embarrassing communications and data.

9. Defendant used the Fruitfly malware to obtain Fruitfly victims' usernames and passwords to third-party websites. Defendant used these stolen credentials to access and download information from these third-party websites including photographs, emails and potentially embarrassing communications and data.

STATUTORY VIOLATIONS

COUNT 1

(Damaging Protected Computer(s), 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B))

The Grand Jury charges:

10. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

11. From in or around 2003 through on or about January 20, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, to wit: the offense caused damage affecting ten (10) or more protected computers during a one (1)-year period, and the offense caused loss to persons during a one (1)-year period from Defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(I) and (VI).

COUNT 2

(Accessing Protected Computer(s), 18 U.S.C. § 1030(a)(2) and (c)(2)(A))

The Grand Jury further charges:

12. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

13. From in or around 2003 through on or about January 20, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally accessed one or more computers without authorization and thereby obtained

information from one or more protected computers, in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(A).

COUNT 3
(Production of Child Pornography, 18 U.S.C. § 2251(a))

The Grand Jury further charges:

14. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

15. From on or about October 25, 2011 through on or about January 14, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did use a minor and minors to engage in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2), for the purpose of producing a visual depiction of such conduct, knowing and having reason to know that such visual depiction would be transported and transmitted, using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce; such visual depiction was produced and transmitted using materials that had been mailed, shipped and transported in and affecting interstate and foreign commerce; and such visual depiction was actually transported and transmitted, using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 2251(a).

COUNTS 4-6
(Wire Fraud, 18 U.S.C. §§ 1343 and 2)

The Grand Jury further charges:

16. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

17. In order to operate the Fruitfly malware, Defendant required access to the computers, storage and internet bandwidth of other individuals and entities infected by or with the Fruitfly malware without their permission or authorization. Defendant required these facilities to, among other things, obfuscate his involvement in operating the Fruitfly malware, provide storage space for the images and files the Fruitfly malware generated, and provide sufficient bandwidth to support the vast amount of information created by the Fruitfly malware.

STATUTORY VIOLATION

18. From in or around August 14, 2011 through on or about January 20, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY devised and intended to devise a scheme and artifice to defraud Fruitfly victims and others, and to obtain money and property, to wit: computer processing power, computer storage, and internet bandwidth and connections, among other things, by means of materially false and fraudulent pretenses, representations and promises.

19. It was part of the scheme that:

a) Defendant obtained and used user credentials and passwords for certain computers infected by the Fruitfly malware to create virtual machines on those Fruitfly victims' computers.

b) Defendant used the computing power and infrastructure of certain Fruitfly victims to spread the Fruitfly malware across the Internet.

c) Defendant used certain Fruitfly victims' computer networks to access sufficient bandwidth to allow the Fruitfly malware to infect protected computers in the Northern District of Ohio, Eastern Division, and elsewhere around the world.

d) Defendant instructed the Fruitfly malware to direct Fruitfly victim computers to report back and, thereafter, send images and files to certain other Fruitfly victims' computers to create repositories of data obtained by the Fruitfly malware. Defendant then remotely accessed these repositories to determine what materials he wanted to preserve in other locations.

e) Defendant created storage containers on certain Fruitfly victims' computers to store and process images and files obtained from other Fruitfly victims.

f) Defendant used certain Fruitfly victims' computers to create proxy networks and servers that obfuscated and hid his role in operating the Fruitfly malware.

20. For the purposes of executing and attempting to execute said scheme and artifice to defraud the Fruitfly victims, and to obtain money and property by means of false and fraudulent pretenses, representations and promises, and attempting to do so, transmitted and caused to be transmitted, by means of wire communications in interstate and foreign commerce, the signals and sounds described below for each count, each transmission constituting a separate count, to wit: various computer program commands and signals between Defendant and various computers in the Fruitfly network as set forth below:

COUNT	APPROXIMATE DATES	DESCRIPTION OF WIRES
4	12/20/2015 – 7/12/2016	Fruitfly malware communications to a computer lawfully controlled by C.B.
5	6/10/2016 – 12/09/2016	Fruitfly malware communications to a computer lawfully controlled by Z.S.
6	12/31/2016 – 01/18/2017	Fruitfly malware communications to a computer lawfully controlled by W.M.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS 7 - 10
(Aggravated Identify Theft, 18 U.S.C. § 1028A(a)(1))

The Grand Jury further charges:

21. The factual allegations of paragraphs 1 through 9 of the General Allegations, and Paragraph 17 of Counts 4 – 6 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

22. On or about the dates listed below, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did knowingly transfer, possess and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit: Wire Fraud, in violation of Title 18, United States Code, Section 1343, knowing that the means of identification belonged to another actual person on or about the dates set forth below:

COUNT	MEANS OF IDENTIFICATION	APPROXIMATE DATES
7	Username and Password for C.B.	August 20, 2014
8	Username and Password for C.B.	August 22, 2014
9	Username and Password for Z.S.	September 7, 2014
10	Username and Password for W.M.	March 29, 2015

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT 11
(Accessing Government Computer Without Authorization, 18 U.S.C. § 1030(a)(3) and (c)(2)(A))

The Grand Jury further charges:

23. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

24. Between on or about May 21, 2014 and on or about December 19, 2016, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY did intentionally, without authorization to access any nonpublic computer of a

department or agency of the United States, access such a computer of that department and agency, Defendant's conduct having affected that use by and for the Government of the United States and said computer was exclusively for the use of the Government of the United States to wit: a computer owned and operated exclusively by a subsidiary of the U.S. Department of Energy, an agency of the United States, in violation of Title 18, United States Code, Sections 1030(a)(3) and (c)(2)(A).

COUNT 12
(Illegal Wiretap, 18 U.S.C. § 2511(1)(b) and (4)(a))

The Grand Jury further charges:

25. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

26. On or about June 25, 2013, between approximately 2:25 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmits a signal through a wire to intercept an oral communication of M.M. and an unknown female, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 13
(Illegal Wiretap, 18 U.S.C. § 2511(1)(b) and (4)(a))

The Grand Jury further charges:

27. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

28. On or about June 23, 2014, between approximately 11:40 a.m. and 11:56 a.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmits a signal through a wire

to intercept an oral communication of J.P. and an unknown male, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 14
(Illegal Wiretap, 18 U.S.C. § 2511(1)(b) and (4)(a))

The Grand Jury further charges:

29. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

30. On or about July 23, 2014, between approximately 7:54 p.m. and 7:57 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmits a signal through a wire to intercept an oral communication of C.A. and an unknown male, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 15
(Illegal Wiretap, 18 U.S.C. § 2511(1)(b) and (4)(a))

The Grand Jury further charges:

31. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

32. On or about March 14, 2015, between approximately 12:20 p.m. and 12:34 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmits a signal through a wire to intercept an oral communication of R.B. and an unknown female, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

COUNT 16
(Illegal Wiretap, 18 U.S.C. § 2511(1)(b) and (4)(a))

The Grand Jury further charges:

33. The factual allegations of paragraphs 1 through 9 of this Indictment are hereby repeated, re-alleged and incorporated by reference as if fully set forth herein.

34. On or about April 11, 2015, between approximately 2:21 p.m. and 2:26 p.m. EST, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendant PHILLIP R. DURACHINSKY intentionally used an electronic device that transmits a signal through a wire to intercept an oral communication of R.B. and an unknown female, in violation of Title 18, United States Code, Sections 2511(1)(b) and (4)(a).

FORFEITURE

The Grand Jury further charges:

The allegations of Counts 1 through 6 and 11 through 16 are hereby realleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982(a)(2)(B); Title 18, United States Code, Section 2253(a)(2); Title 18, United States Code, Section 2253(a)(3); Title 18, United States Code, Section 981(a)(1)(C); Title 28, United States Code, Section 2461(c); Title 18, United States Code, Section 1028(b)(5); and, Title 18, United States Code, Section 2513; Title 28, United States Code, Section 2461(c). As a result of the foregoing offenses, Defendant PHILLIP R. DURACHINSKY shall forfeit the following to the United States:

a. All property constituting, or derived from, proceeds he obtained directly or indirectly as a result of the violations charged in Counts 1, 2 and 11.

b. All property, real or personal, constituting or traceable to gross profits or other proceeds obtained from the violation charged in Count 3; and any property real or

personal, used or intended to be used, to commit or to promote the commission of the violation charged in Count 4 and any property traceable to such property.

c. All property, real or personal, which constitutes or is derived from proceeds traceable to the violations charged in Counts 4, 5 and 6.

d. Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in the violations charged in Counts 12, 13 14, 15 and 16.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.